IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF: **EVIDENCE LOCATED AT:** **UNITED STATES PROBATION** **700 GRANT STREET** **PITTSBURGH, PA 15219**	Case No. 21-mj-964

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, J. Brandon Wargo, a Special Agent (SA) with the Homeland Security Investigations, being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. This affidavit supports an application for a search warrant that seeks authorization to seize and search evidence that has already been seized by the Probation Office. As shown in more detail below, the Probation Office seized a laptop during a home visit. The Probation Office submitted that laptop to one of its forensic analysts for testing. The Probation Office located images on the laptop that appear to be images of child exploitation. To further investigate any potential wrongdoing, law enforcement officers seek authorization to seize that laptop and copies of any digital copies that have been created. The Probation Office currently has custody of all of the evidence that the warrant seeks authorization to seize and search. The Probation Office is holding the evidence at 700 Grant Street, Pittsburgh, PA, 15219. The evidence is described in more detail below and in Attachment A. The materials that law enforcement officers seek to seize from that property is described in more detail below and in Attachment B.

AGENT BACKGROUND

2. I am a Special Agent with the Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), and I am currently assigned to the Pittsburgh, Pennsylvania Office. I have been so employed since June 2009.

3. As part of my duties as an HSI Special Agent, I investigate criminal violations relating to high technology crime, cyber-crime, child exploitation and child pornography, including violations pertaining to the illegal distribution, receipt, possession, and production of materials depicting the sexual exploitation of children in violation of Title 18, United States Code, Sections 2252(a)(2), 2252(a)(4)(B) and 2251, and Title 18, United States Code, Sections 2423(b), and 2423(c) as they relate to travel to engage in illicit sexual contact with a minor.

4. I have received training in the area of child pornography and child exploitation investigations and have had the opportunity to observe and review numerous examples of such materials in a variety of electronic media.

5. I am a member of the Pennsylvania Internet Crimes Against Children (ICAC) Task Force and the Western Pennsylvania Crimes Against Children Task Force (WPCACTF). I have participated in and led numerous child pornography investigations. I have executed numerous search warrants related to child pornography investigations. In this regard, I have reviewed extensive samples of child pornography, including videos, photographs, and digital reproductions of photographs or other print media.

TARGET OFFENSE(S) AND PROPERTY TO BE SEIZED/SEARCHED

6. This affidavit is made in support of an application for a search warrant for evidence held at the United States Probation Office, 700 Grant Street, Pittsburgh, PA 15219 in the investigation of ANDREW KINCAID, for items specified in Attachment B. The evidence is specifically described in Attachment A.

7. The property to be searched (hereinafter "TARGET DEVICES") is described as follows:

a. ASUS Gaming A15 (Model: TUF506, Serial Number: LANRCX05D13244) (hereinafter "ASUS Gaming Laptop"); and

b. Any medium or device containing any data previously forensically extracted from the ASUS Gaming Laptop.

8. The TARGET DEVICES are currently located at the United States Probation Office, 700 Grant Street, Pittsburgh, PA 15219.

9. The purpose of this application is to seize evidence, fruits and instrumentalities, more particularly described in Attachment B, of a violation of Title 18, United States Code, Section 2252, pertaining to the illegal distribution, receipt, and possession of child pornography.

FACTS RELATING TO PROBABLE CAUSE

10. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, contraband, and instrumentalities of the

violations of Title 18, United States Code, Section 2252 are presently located on the evidence held at the United States Probation Office in Pittsburgh, PA. I request authority to search the entirety of the TARGET DEVICES, for the items specified in Attachment B, hereto, which items constitute fruits, contraband, instrumentalities, and evidence of the foregoing violations.

11. The statements in this affidavit are based on: (A) my investigation of this matter, (B) information provided by other sworn law enforcement officers and other personnel specially trained in the seizure and analysis of computers, electronic mobile devices, and electronic storage devices; and (C) my experience and training as a special agent.

12. On or about March 16, 2021, United States Probation Officer (USPO) for the Western District of Pennsylvania, Timothy Lentz, conducted a random home inspection of ANDREW KINCAID's residence. Per reporting provided by the USPO, during the visit, a power cord was observed plugged into the wall next to KINCAID's desk. When questioned about the cord, KINCAID admitted to possessing a laptop computer that was not monitored or reported to the probation office. KINCAID also reported that he had the device in his possession an estimated three months and that he did use the internet to view adult pornography.

13. The Probation Officer seized the laptop. The laptop that the Probation Officer seized is the laptop that I described as the ASUS Gaming Laptop.

14. Per the USPO, KINCAID was subject to the following conditions of probation, which were in effect at the time of the home visit that occurred on March 16,

2021, and were the basis for KINCAID's probation revocation, the petition for which was filed on or about April 15, 2021:

a. **Mandatory Condition:** You must not commit another federal, state, or local crime.

b. **Special Condition 6:** The defendant shall not possess any materials, including pictures, photographs, books, writings drawings, videos, or video games depicting and/or describing "child pornography" as defined at 18 U.S.C. § 2256(8).

c. **Special Condition 10:** The defendant shall provide the U.S. Probation Office with accurate information about his entire computer system and shall abide by the Computer Restriction and Monitoring Program.

d. **Special Condition 16:** For the ten years following August 13, 2019, the defendant may not own or use a computer or internet connected device, except he may use such while in the probation office or elsewhere in the presence of a probation office employee. The defendant may also use "point of sale" retail or ATM devices for regular commercial transactions, even if connected to the internet. He may also possess and use a non-internet cellphone for voice calls only. Any use of a computer or internet-connected device permitted by this paragraph 16 must comply with conditions 8, 9, and 10 of ECF NO. 55, and the computer restrictions and monitoring program rules and participant agreement signed by the defendant dated April 8, 2019.

15. On or about March 17, 2021, USPO Lentz requested a forensic examination be conducted of the ASUS Gaming Laptop. The ASUS Gaming Laptop was sent to Richard Wactor, a forensic examiner for the United States Probation Office.

16. On or about April 13, 2021, forensic examiner Wactor provided a report to USPO Lentz. The report detailed his forensic analysis of the ASUS Gaming Laptop and his discovery of over 500 images of child sexual abuse material (child pornography), as well as images of animated child sexual abuse material. Documented within Wactor's report are the following descriptions of three located files:

a. The first image, identified as MD5 Hash value 39eef326d76e930149cc53b1c7a6ddb5, depicts a prepubescent minor female lying down on her back as an adult male is penetrating her with his penis. The female is wearing only a shirt, which she has pulled up to expose the lower portion of her body.

b. The second image, identified as MD5 Hash value 5fa0d4d4a6c9781a7df1a311d41e15c9, appears to be an android screen capture and depicts a nude prepubescent minor female (toddler) sitting up with her legs spread apart exposing her vagina in a lascivious manner, with what appears to be semen around her vagina.

c. The third image, identified as MD5 Hash value 9f4818c77920d002160035bb2ecf6bdf, depicts a partially nude prepubescent minor female reclined with her dress pulled up, as a male is penetrating her with his penis.

17. On or about April 23, 2021, your affiant was initially advised of the aforementioned information and was requested to assist in the investigation.

18. On or about April 28, 2021, your affiant received case information from the United States Attorney's Office, which included reporting prepared by the United States Probation Office and the results of the preliminary forensic examination conducted by the United States Probation Office.

19. On or about April 30, 2021, your affiant reviewed docket number 2:09-CR-00230-MRH, specifically ECF entry number 55, the Judgement in the criminal case against KINCAID. That document, under "Additional Supervised Release Terms," stated the following:

> Defendant is permitted to possess and/or use a computer and is permitted access to the internet. However, defendant is not permitted to use a computer or other electronic communication or data storage devices, including a cell phone, to access child pornography or to communicate with any individual or group for the purpose of promoting sexual relations with children. Defendant shall consent to the installation of any hardware/software to monitor any computer or other electronic communication or data storage devices used by defendant to confirm his compliance with this condition. Defendant shall pay the monitoring costs as directed by the probation officer. Further, defendant shall consent to periodic unannounced examinations by the probation officer of any computers, cell phones or other electronic communication or data storage devices that defendant has access to in order to confirm defendant's compliance with this condition. Additionally, defendant shall consent to the seizure and removal of hardware and data storage media for further analysis by the probation officer based upon reasonable suspicion of a violation of the conditions imposed in this case or based upon reasonable suspicion of unlawful conduct by defendant. Defendant's failure to submit to the monitoring and search of computers and other electronic communication or data storage devices used by him may be grounds for revocation.

20. On or about April 30, 2021, your affiant reviewed 2:09-CR-00230-MRH, specifically ECF entry number 121, which was a modification of conditions of supervised

release. The document was signed by KINCAID on or about August 27, 2020. The document again restricted his use of computers and other electronic devices and referenced the conditions annotated in ECF entry number 55 (as previously documented in this affidavit).

DEFINITIONS

21. The following definitions apply to this Affidavit and Attachment B to this Affidavit:

a. "**Minor**," as defined in 18 U.S.C. § 2256(1), means any person under the age of 18 years.

b. "**Child Erotica**," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

c. "**Child Pornography**," as used herein, includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct) as well as any visual depiction the production of which involves

the use of a minor engaged in "sexually explicit conduct," as that term is defined in 18 U.S.C. § 2256(2).

d. "**Visual depictions**" include undeveloped film and videotape, data stored on computer disk or by electronic means, which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format. *See* 18 U.S.C. § 2256(5).

e. "**Sexually explicit conduct**" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any persons. *See* 18 U.S.C. § 2256(2).

f. A "**wireless telephone**" (or mobile telephone or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text

messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

g. "**Computer**," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1), as an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

h. A "**digital camera**" is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

i. "**Internet Service Providers**" or "**ISPs**," are businesses that enable individuals to obtain access to the Internet. ISPs provide their customers with access to the Internet using telephone or other telecommunications

lines, provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers, remotely store electronic files on their customers' behalf, and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or businesses that have subscriber accounts with them. Those records often include identifying and billing information, account access information in the form of log files, electronic mail transaction information, posting information, account application information, and other information both in computer data and written format.

j. An "**Internet Protocol**" or "**IP**" address is a unique numeric address used by computers or cellular telephones on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer connected to the Internet must have an assigned IP address so that Internet traffic sent from and directed to that computer may be properly directed from its source to its destination. Most ISPs control a particular range of IP addresses. When a customer connects to the Internet using an ISP service, the ISP assigns the computer an IP address. Any and all computers using the same ISP account during that session will share an IP address. The customer's computer retains the IP address for the duration of the Internet session until the user disconnects. The IP address cannot be assigned to a user with a different ISP account during that session. When an Internet user

visits any website, that website receives a request for information from that customer's assigned IP address and sends the data to that IP address, thus giving the Internet user access to the website.

k. The "**Internet**" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

FORENSIC ANALYSIS

22. Based on my training, experience, and research, I know that laptop computers, desktop computers, and hard drives, allow for the storage of large amounts data, including internet browsing histories, documents, images, and videos. They also function as a repository for backing up data from cellular telephones, namely images and video files. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

23. In my training and experience, I know that computers and electronic mobile devices essentially serve four functions in connection with child pornography: (1) production; (2) communication; (3) receipt/distribution; and (4) storage.

24. Child pornographers can now easily transfer existing hard copy photographs into a computer-readable format with a scanner. With the advent of digital cameras, images can be transferred directly from the digital camera onto an electronic

mobile device or a computer. Moreover, a device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

25. The Internet affords collectors of child pornography several different venues for obtaining, viewing, and distributing child pornography in a relatively secure and anonymous fashion. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by internet portals such as Google, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in a variety of formats. A user can set up an online storage account from any computer or device with access to the Internet. Evidence of such online storage of child pornography is often found in the user's computer.

26. A computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store hundreds of thousands of images at very high resolution.

27. With the advent of smart phones and advanced technology, cellular telephones and other electronic mobile devices function as "computers" in the sense that they can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. In fact, some cellular telephones are equipped with memory or SIM cards, which are compact removable

storage devices commonly used to store images and other electronic data that can be inserted into a telephone's camera as well as other small digital devices such as tablet devices or hand held computers. Much like "thumb drives," some memory cards have the ability to store large amounts of electronic data, including thousands of images or videos, and on occasion entire operating systems or other software programs. Moreover, cellular telephones offer a broad range of capabilities. In addition to enabling voice communications and containing a "call log" that records phone call details, cellular telephones offer the following capabilities: storing names and phone numbers in electronic "address books;" sending receiving, and storing text messages and e-mails; taking, sending, receiving, and storing still photographs and moving videos; storing and laying back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet.

28. Communications made by way of computer or electronic mobile devices can be saved or stored on the items used for these purposes. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or electronic mobile device, or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally. For example, traces of the path of an electronic communication may be automatically stored in many places like temporary files or Internet Service Provider client software. In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner can often recover evidence which shows that a computer or electronic mobile device contains peer to peer software, when the computer was sharing files, and

even some of the files that were uploaded or downloaded. Such information may be maintained indefinitely until overwritten by other data.

29. Computer and electronic mobile device users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer and electronic mobile device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer and electronic mobile device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." By using steganography, a computer or electronic mobile device user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband, or instrumentalities of a crime.

30. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive or other electronic storage media, deleted or viewed via the Internet. Electronic files saved to a hard drive or electronic storage media can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensics tools. Normally, when a person deletes a file on a computer or electronic mobile device, the data contained in the file does not actually disappear; rather,

that data remains on the hard drive or electronic storage media until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space (i.e., space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space for long periods of time before they are overwritten).

31. In addition, a computer's (or electronic mobile device's) operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive or electronic storage media depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer or electronic mobile device habits. A substantial amount of time is necessary to extract and sort through data in this free or unallocated space.

32. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processor, picture, and movie files), computers and electronic mobile devices can contain other forms of electronic evidence as well. In particular, records of how a computer or electronic mobile device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the computer and electronic mobile devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital

data that can be neatly segregated from the hard drive image as a whole. Digital data on the hard drive or electronic storage media not currently associated with any file can provide evidence of a file that was once on the hard drive or electronic storage media but has since been deleted, edited, or deleted in part such as a word processing file with a deleted paragraph. Virtual memory paging systems can leave digital data on the hard drive or electronic storage media that show what tasks and processes on the computer or electronic storage media were recently used. Web browsers, e-mail programs, and chat programs store configuration data on the hard drive or electronic storage media that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer or electronic mobile device was in use. Computer file systems (or those on electronic mobile devices) can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations.

33. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

34. **Forensic evidence.** As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how each device was used, the purpose of its use, who used it, and when.

There is probable cause to believe that this forensic electronic evidence might be on each device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited; virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled a device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be

merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the device and the application of knowledge about how a device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

35. **Nature of examination.** Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the later examination of the devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

36. **Manner of execution.** Because this warrant seeks only permission to examine devices and forensic extractions already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CHARACTERISTICS COMMON TO INDIVIDUALS: (1) INVOLVED IN RECEIVING CHILD PORNOGRAPHY; AND/OR (2) WHO HAVE A SEXUAL INTEREST IN CHILDREN AND IMAGES OF CHILDREN

37. Based on my previous investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that individuals who view and receive multiple visual depictions of minors engaged in sexually explicit conduct are often individuals who have a sexual interest in children and in images of children, and I know that there are certain characteristics common to such individuals:

a. Such individuals almost always possess and maintain their "hard copies" or "digital copies" of child sexual abuse material (child pornography)—that is, their pictures, photographs, digital images/videos, correspondence, etc. in some private and secure location, and they typically retain this material for many years. Often, such individuals maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer or electronic mobile device. These collections are often maintained for several years and are kept close by, to enable the individual to easily view the collection, which is valued highly.

b. Such individuals also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

c. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

38. In my training and experience, the Internet affords collectors of child sexual abuse material (child pornography) several different venues for obtaining viewing and distributing child pornography in a relatively secure and anonymous fashion. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by internet portals such as Google, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in a variety of formats. A user can set up an online storage account from any computer or device with access to the Internet. Evidence of such online storage of child pornography is often found in the user's computer, including personal computers, such as cellular telephones.

39. Because of the advanced technology and growing capability of cellular telephones to function as computers and the characteristics of individuals interested in child sexual exploitation material, as described above, it is your affiant's experience that individuals who collect, receive and distribute images of child sexual abuse material, commonly do so on their cellular devices.

CONCLUSION

40. Based on the aforementioned factual information, your affiant respectfully submits that there is probable cause to believe that evidence, fruits and instrumentalities of violations of Title 18, United States Code, Section 2252 may be located on the TARGET DEVICES described in Attachment A.

41. Your affiant, therefore, respectfully requests that the attached warrant be issued authorizing the search for the items listed in Attachment B.

* * *

The above information is true and correct to the best of my knowledge, information, and belief.

/s/ J. Brandon Wargo
J. Brandon Wargo
Special Agent
Homeland Security Investigations

Sworn and subscribed to me,
by telephone pursuant to
Fed. R. Crim. P. 4.1(b)(2)(A),
this 5th day of May, 2021.

The Honorable Maureen P. Kelly
United States Magistrate Judge

ATTACHMENT A

1. This Attachment describes the property to be seized and searched. The items to be seized and searched are as follows:

a. ASUS Gaming A15 (Model: TUF506, Serial Number: LANRCX05D13244) (the "ASUS Gaming Laptop"); and

b. Any medium or device containing any data previously forensically extracted from the ASUS Gaming Laptop.

2. All of the property to be seized and searched is in the custody of the Probation Office in the Western District of Pennsylvania located at 700 Grant Street, 2nd Floor, Pittsburgh, PA 15219.

ATTACHMENT B

1. This Attachment describes the property, materials, and/or information that will be seized from the property described in Attachment A.

2. In particular, the warrant seeks authorization to seize any and all fruits, contraband, records, evidence and instrumentalities on the TARGET DEVICES, as described in Attachment A, that relate to violations of Title 18, United States Code, Sections 2252(a)(2) and 2252(a)(4)(B) (Receipt and Possession of Child Pornography) and involve ANDREW KINCAID, including:

a. Records and information, including photos, images, and videos, constituting, referencing, or revealing child pornography, child erotica, or any erotic, pornographic, or nude images and/or videos as they relate to the crimes under investigation;

b. Child erotica and evidence of access to children;

c. Information, correspondence, records, documents or other materials constituting evidence of or pertaining to child pornography, child erotica, or access to children; or constituting evidence of or pertaining to the possession and receipt, accessing, or transmission through interstate or foreign commerce of child pornography, child erotica, or visual depictions of minors engaged in sexually explicit conduct; or constituting evidence of or pertaining to an interest in child pornography or sexual activity with children;

d. Records or documents evidencing occupancy or ownership of the ASUS Gaming Laptop, including utility and telephone bills, email or addressed correspondence;

e. Evidence of who used, owned, or controlled the ASUS Gaming Laptop at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

f. Evidence of software that would allow others to control the ASUS Gaming Laptop, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

g. Evidence of the lack of such malicious software;

h. Evidence of the attachment to the ASUS Gaming Laptop of other storage devices or similar containers for electronic evidence;

i. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the ASUS Gaming Laptop;

j. Evidence of the times the ASUS Gaming Laptop was used;

k. Records of or information about the ASUS Gaming Laptop's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered

into any Internet search engine, and records of user-typed web addresses; and

l. contextual information necessary to understand the evidence described in this attachment.

3. In searching the TARGET DEVICES, the federal agents may examine all of the information contained in the TARGET DEVICES to view their precise contents and determine whether the information falls within the items to be seized as set forth above. In addition, they may search for and attempt to recover "deleted," "hidden," or encrypted information to determine whether the information falls within the list of items to be seized as set forth above.

4. As used above, the terms "records" and "information" includes all forms of creation or storage, including any of the following:

a. Any form of computer or electronic storage (such as hard disks or other media that can store data);

b. Text messages or similar messages such as SMS or IM, saved messages, deleted messages, draft messages, call logs, all phone settings (*i.e.* call, messaging, display), priority senders, photographs, videos, links, account information, voicemails and all other voice recordings, contact and group lists, and favorites;

c. Pictures, all files, cloud files and relevant data without password access, storage information, documents, videos, programs, calendar information, notes, memos, word documents, PowerPoint documents, Excel Spreadsheets, and date and time data;

d. Payment information, to include account numbers, names, addresses, methods of payment, amounts, additional contact information, and financial institutions;

e. Lists and telephone numbers (including the number of the phone itself), names, nicknames, indicia of ownership and/or use, and/or other contact and/or identifying data of customer, co-conspirators, and financial institutions;

f. Applications (Apps), to include subscriber information, provider information, login information, contact and group lists, favorites, history, deleted items, saved items, downloads, logs, photographs, videos, links, messaging or other communications, or other identifying information;

g. Social media sites to include, name and provider information of social media network(s), profile name(s), addresses, contact and group lists (*i.e.* friends, associates, etc.), photographs, videos, links, favorites, likes, biographical information (*i.e.* date of birth) displayed on individual page(s), telephone numbers, email addresses, notes, memos, word documents, downloads, status, translations, shared information, GPS, mapping, and other information providing location and geographical data, blogs, posts, updates, messages, or emails;

h. Any information related to co-conspirators (including names, addresses, telephone numbers, or any other identifying information);

i. Travel log records from GPS data (*i.e.* Google Maps and/or other Apps), recent history, favorites, saved locations and/or routes, settings, account information, calendar information, and dropped pinpoint information;

j. Internet service provider information, accounts, notifications, catalogs, Wi-Fi information, search history, bookmarks, favorites, recent tabs, deleted items and/or files, downloads, purchase history, photographs, videos, links, calendar information, settings, home page information, shared history and/or information, printed history and/or information, or location data; and

k. Email data, including email addresses, IP addresses, DNS provider information, telecommunication service provider information, subscriber information, email provider information, logs, drafts, downloads, inbox mail, sent mail, outbox mail, trash mail, junk mail, contact lists, group lists, attachments and links, and any additional information indicative of the above-specified offenses.